10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

**~~ Patent Literature Abstracts**

12/3,K/2 (Item 2 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0016657393 *Drawing available*
WPI Acc no: 2007-372480/200735
XRPX Acc No: N2007-277727
**Namespace server for data processing system, has network attached storage network redirecting redirection-capable client` s access, and processor coupled to memory for accessing translation information and protocol information**
Patent Assignee: FAIBISH S (FAIB-I); FRIDELLA S A (FRID-I); GUPTA U K (GUPT-I); JIANG X (JIAN-I); STACEY C H (STAC-I); WURZL M (WURZ-I); ZIMRAN E (ZIMR-I)
Inventor: FAIBISH S; FRIDELLA S A; GUPTA U K; JIANG X; STACEY C H; WURZL M; ZIMRAN E

Patent Family ( 1 patents, 1 countries )

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---|---|---|---|---|---|---|---|
| US 20070055703 | A1 | 20070308 | US 2005221011 | A | 20050907 | 200735 | B |

Priority Applications (no., kind, date): US 2005221011 A 20050907

Patent Details

| Patent Number | Kind | Lan | Pgs | Draw | Filing Notes |
|---|---|---|---|---|---|
| US 20070055703 | A1 | EN | 40 | 27 | |

**Alerting Abstract** ...NOVELTY - The server (44) has a memory for storing translation information for translating pathnames in a **client**-server network (21) to respective translated pathnames and storing protocol **information** defining file **access** protocols. A processor is coupled to the memory for **accessing** the translation **information** and the protocol information. The processor is programmed for receiving requests from the **clients** for access to files referenced by the pathnames. A network attached storage (NAS) network redirects a redirection-capable **client**` s access back to the namespace server. ... a data processing system comprising a namespace server a method of **request** redirection in a **data** processing system...

**Original Abstracts:**A namespace server translates **client** requests for access to files referenced by pathnames in a **client**-server namespace into requests for access to files referenced by pathnames in a NAS network namespace. The namespace server also translates between different file access protocols. If a **client** supports redirection and is requesting access to a file in a file server that supports the **client**'s redirection, then the namespace server may redirect the **client** to the NAS network pathname of the file. Otherwise, the namespace server forwards a translated **client** request to the file server, and returns a reply from the file server to the **client**. A file server may redirect a redirection-capable **client**'s access back to the namespace server for access to a share, directory, or file that is offline for migration, or for a deletion or name change that would **require** a change in translation **information** in the namespace server.

**Claims:**What is claimed is:**1**. A multi-protocol namespace server for providing a unified **client**-server network namespace to **clients** using different file access protocols to access files in **different** file **servers** in a network attached storage (NAS) network namespace, some of the **clients** using file access protocols that support redirection and others of the

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

**clients** using file access **protocols** that do **not support** redirection, and some of the file servers supporting file access **protocols** that are **not supported** by others of the file servers, said multi-**protocol** namespace server comprising:memory for storing translation information for translating pathnames in the **client**-server network namespace to respective translated pathnames in the NAS network namespace and for storing protocol **information** defining file **access** protocols for accessing files at the respective translated pathnames in the NAS network namespace, andat least one processor coupled to the memory for **accessing** the translation **information** and the protocol information, said at least one processor being programmed for receiving requests from the **clients** for access to files referenced by pathnames in the **client**-server network namespace and translating the pathnames in the **client**-server network namespace to respective translated pathnames in the NAS network namespace, and for responding to some of the requests from said some of the **clients** by returning redirection replies to said some of the **clients**, the redirection replies including translated pathnames in the NAS network namespace, and for responding to the requests from said others of the **clients** by forwarding translated requests to the file servers, the translated requests including translated pathnames in the NAS network namespace, and for translating and forwarding a request of a **client** supporting redirection for access to a file upon determining that the file to be accessed by the **client** supporting redirection is stored in a file server that does not support redirection from the **client** supporting redirection.

12/3,K/3 (Item 3 from file: 350) (Note current app)

0014884267 *Drawing available*
WPI Acc no: 2005-232006/200524
XRPX Acc No: N2005-191109
**Data generating method for use in web server, involves sending request from secondary server to primary server to obtain data from client in response to finding need for data that results from using communication protocol**
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: BURROWS W L; KARIOTH G; MORAN A S; PFITZMANN B M; SCHUNTER M; TURNER B J

Patent Family ( 1 patents, 1 countries )

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---|---|---|---|---|---|---|---|
| US **20050055434** | A1 | 20050310 | US 2003655368 | A | 20030904 | 200524 | B |

Priority Applications (no., kind, date): US 2003655368 A 20030904

Patent Details

| Patent Number | Kind | Lan | Pgs | Draw | Filing Notes |
|---|---|---|---|---|---|
| US 20050055434 | A1 | EN | 15 | 5 | |

**Alerting Abstract** ...NOVELTY - The method involves sending a request from a secondary server (204) to a primary server (202) to **obtain data** from a **client** in response to finding the **need** for **data** that results from using a communication protocol. The primary server executes the protocol/delegates execution of the protocol to a third server to **obtain** the resulting **data**. Processing associated with another **request** is continued using the resulting data. ... of certain communication protocols within other server-side components that have the ability to achieve interaction with users through web browsers and similar types of

**client applications**. The method provides the ability to **integrate certain** protocols into server-side components, **applications** infrastructure. The method allows the server-side **component** to obtain the functionality or the results of executing a restricted protocol and allows implementation of the protocol within a different server-side component... ... 206Communication protocol **data requirement** detection unit

**Original Abstracts:**A method is presented for **obtaining information** from a **client for** the benefit **of** a server using a particular communication **protocol** that the server **does not implement**. A primary **server receives** a **client**-generated request, and **the** primary server sends a first **request** to a **secondary server** as part **of the** processing of the **client**-generated request. While **processing** the first request, the **secondary** server determines a need **for** data obtainable from a client application that supports user interaction using a communication protocol for which the **secondary server** is not **configured to** implement. The **secondary server** sends a **second request** to the **primary server** for obtaining data that results from using the communication protocol. The **secondary server** subsequently receives **the resulting** data and continues to **process** the first **request** using the resulting **data**, after which the **secondary** server returns a response for the first request to the primary server.

...**Claims:**generating data at a server, the method comprising:receiving at a secondary server from a primary server a first request that is based on a **client**-generated request from a **client**;while processing the first request **at** the **secondary** server, determining at the secondary server a need for data that is obtainable from a client application at the client using a communication protocol for which the **secondary server** is not configured to implement; andin response to determining the **need for** data that results from using the communication protocol, sending from the **secondary server** to the primary **server** a **second** request for obtaining data from the client **that results** from using the **communication** protocol, **wherein the** primary **server executes** the communication **protocol** or delegates execution of the communication protocol to a third server to **obtain** the resulting **data**;in response to sending the second request, receiving at the secondary **server** from the **primary** server the resulting **data**;in response to receiving **the** resulting **data**, continuing processing that is associated with the first **request using** the resulting **data**; andreturning from the secondary server to the primary server a response for the **first request.**

12/3,K/5 (Item 5 from file: 350)

0010864418 *Drawing available*
WPI Acc no: 2001-483506/200152
XRPX Acc No: N2001-357878
**Computer network for authenticating and authorizing users accessing network of computer systems has server of first sub-network that passes at least some authentication requests through second encrypted protocol handier**
Patent Assignee: SUN MICROSYSTEMS INC (SUNM)
Inventor: LIMSICO C T

| Patent Family ( 4 patents, 93 countries ) | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Patent Number** | **Kind** | **Date** | **Application Number** | **Kind** | **Date** | **Update** | **Type** |
| WO 2001057626 | A2 | 20010809 | WO 2001US2353 | A | 20010124 | 200152 | B |
| AU 200131123 | A | 20010814 | AU 200131123 | A | 20010124 | 200173 | E |

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| EP 1252752 | A2 | 20021030 | EP 2001903287 | A | 20010124 | 200279 | E |
| | | | WO 2001US2353 | A | 20010124 | | |
| US 6662228 | B1 | 20031209 | US 2000495565 | A | 20000201 | 200381 | E |

Priority Applications (no., kind, date): US 2000495565 A 20000201

| Patent Details | | | | | | |
|---|---|---|---|---|---|---|
| **Patent Number** | **Kind** | **Lan** | **Pgs** | **Draw** | **Filing Notes** | |
| WO 2001057626 | A2 | EN | 21 | 3 | | |
| National Designated States,Original | AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW | | | | | |
| Regional Designated States,Original | AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW | | | | | |
| AU 200131123 | A | EN | | | Based on OPI patent | WO 2001057626 |
| EP 1252752 | A2 | EN | | | PCT Application | WO 2001US2353 |
| | | | | | Based on OPI patent | WO 2001057626 |
| Regional Designated States,Original | AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR | | | | | |

**Alerting Abstract** ...encrypted protocol passes information between the communications channel and a second authentication server (210). The server of the first sub-network passes at least some **authentication requests** through the second encrypted protocol handler, the firewall, the communications channel, and the first encrypted protocol handler to the second authentication server.

**Original Abstracts:**first authentication server, a firewall, and network interconnect. This subnetwork is connected through encrypted protocol handlers and over a potentially insecure channel to a second **authentication** server. Some **authentication requests**, especially for **users not** authenticated in the first **authentication** server's database and determined by the first authentication server to be authenticatable by the second authentication server, are passed from the server of the... ... first authentication server, a firewall, and network interconnect. This subnetwork is connected through encrypted protocol handlers and over a potentially insecure channel to a second **authentication** server. Some **authentication requests**, especially for users not **authenticated** in the **first authentication** server's database and determined by the first authentication server to be authenticatable by the second authentication server, are passed from the server of the... ... a first authentication server, a firewall, and network interconnect. This subnetwork is connected through encrypted protocol handlers and over a potentially insecure channel to a **second** authentication **server**. Some **authentication requests**, especially for users **not** authenticated in the first **authentication server's** database **and determined** by the first **authentication** server to be authenticatable by **the second** authentication **server**, are passed from the server of the subnetwork through the encrypted protocol handlers and over the potentially insecure channel to the second authentication server...
...**Claims:**firewall;upon receiving a login attempt to the first server, determining that the login attempt is of type permitted to be authorized by the second **authorization**

server;passing an **authentication request** through the first encrypted protocol handler, the first firewall, the second firewall, and the second **encrypted protocol** handler to the second **authorization** server; andpassing password, challenge and response information between the second authorization server and the first server to authenticate the login attempt,wherein determining that...

19/3,K/1 (Item 1 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0015765813 *Drawing available*
WPI Acc no: 2006-327270/200634
XRPX Acc No: N2006-277052
**File service operation providing method used in computing network, involves providing virtual interface discriminator to clients accessing failed sever to allow clients to access another sever of network**
Patent Assignee: NETWORK APPLIANCE INC (NETW-N)
Inventor: SCOTT J A

| Patent Family ( 1 patents, 1 countries ) | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Patent Number** | **Kind** | **Date** | **Application Number** | **Kind** | **Date** | **Update** | **Type** |
| US 7039828 | B1 | 20060502 | US 200286657 | A | 20020228 | 200634 | B |

Priority Applications (no., kind, date): US 200286657 A 20020228

| Patent Details | | | | | |
|---|---|---|---|---|---|
| **Patent Number** | **Kind** | **Lan** | **Pgs** | **Draw** | **Filing Notes** |
| US 7039828 | B1 | EN | 17 | 7 | |

**Alerting Abstract** ...ownership of set of storage device owned by file sever which is detected to suffer from error condition. A virtual interface discriminator is set to **client** (104) accessing the failed sever. The failover **clients** is allowed to access error free sever by computing network address associated with the sever from symbolic name generated from symbolic name of failed sever. ... ADVANTAGE - The failover sever is allowed to receive **requests** from **clients** accessing the failover sever by providing a virtual interface discriminator to the **client**, therefore efficiency of the network is improved...

**Original Abstracts:**A system and method for clustered failover over transport media that does **not support** moving of transport addressed between network interface controllers is provided. This reviving file server of a cluster, upon detection of the failure of its partner, assumes ownership of the disks owned by the failed file server. The surviving file **server** activates a **secondary** discriminator or port for access by **clients** who normally utilized the failed file server. **Clients** generate the name of the surviving or failover file server by appending at set item to the name of the failed file server.

**Claims:**What is claimed is:1. A method for a **first** file **server** to provide file service operations normally performed by a **second** file **server** after the **second** file **server** suffers an error condition, the first and **second** file **servers** operatively interconnected with a set of **clients** using a network **protocol**, the network **protocol** being free of support for moving a transport address from the **second** file **server** to the **first** file **server**, the method comprising the steps of:detecting, by the **first** file **server**, that the **second** file **server** has suffered an error condition;asserting ownership, by the **first** file **server**, of a

set of storage devices normally owned by the **second** file **server**;activating, on the **first** file **server**, a **secondary data access** port for receiving connections over a network; andprocessing, by the **first** file **server**, file service operations directed to the secondary **data access** port from a set of failover **clients**, the failover **clients** accessing the **first** file **server** by computing a network address associated with the **first** file **server** from a **first** symbolic name, the first symbolic name generated by the failover **client** from a second symbolic name associated with the **second** file **server**, whereby failover operation is achieved by the **client.**

19/3,K/2 (Item 2 from file: 350)

0015277852 *Drawing available*
WPI Acc no: 2005-627975/200564
XRPX Acc No: N2005-515564
**Consumer device operating method e.g. desktop computer, involves connecting device to remote system through intermediated hidden agent transfer protocol servers by communication links**
Patent Assignee: AMAZON.COM INC (AMAZ-N)
Inventor: KRONZ J A

Patent Family ( 1 patents, 1 countries )

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---|---|---|---|---|---|---|---|
| US 6941374 | B1 | 20050906 | US 1999369114 | A | 19990805 | 200564 | B |

Priority Applications (no., kind, date): US 1999369114 A 19990805

Patent Details

| Patent Number | Kind | Lan | Pgs | Draw | Filing Notes |
|---|---|---|---|---|---|
| US 6941374 | B1 | EN | 17 | 4 | |

**Alerting Abstract** ...NOVELTY - The method involves forming a link between the first consumer device with the **first** intermediate **server**. Authorization is carried out between the first and **second** intermediate **server**, ensuring that the first device has the access right to access the services of the remote device. Once a link has been established, a connection is made between the **second** intermediate **server** and the **second** remote device, forming a transparent link between first and second device. The first device **requests** from the **first** intermediate **server** a listing of the services available from the second device. ... Server An apparatus for accessing services A method for accessing remote services by **client** device A **client** apparatus A **system** for communicating **client** devices ... ... device such as desktop computers, personal digital assistants (PDA), laptop computer, notebook computer, embedded processor devices, printers, fax, machines, scanners, remote control units, X-to^ **T^ M** type electrical control devices, thermostats electrical outlets, light switches, window controls, garage door systems, whole house control systems, heating ventilation air conditioning (HVAC) systems, security... ... ADVANTAGE - Enables accessing remote services of consumer devices by extending the functionality of the Service Discovery Transfer **protocol**.**Title Terms** .../Index Terms/Additional Words:

**Original Abstracts:**method for a first device to access the services supplied by a second device by establishing a communicative connection between the first consumer device and **a**

first server. The first server, establishes a communicative connection between the first **server** and a **second server**. The **second server establishes** a **communicative connection** between the **second server** and the **second device**. Once the **communicative** connection are established, a service **request** can be sent **from** the first device, to the second device utilizing the communicative connections. In response to receiving the **request** the second consumer **device** can perform the **requested** service.

**Claims:**20. A system for allowing **client** devices **remote** from each other to **communicate** via intermediate **server** devices, the system comprising:a local server able to communicatively couple to a **client** device that is **local** to the local server, the local **client** device designed to **communicate** only with other local **client** devices, **the** local **server** also able to communicatively couple to a remote server, the local server operative to:receive a **request** from the local **client** device **for** an indicated service **to** be performed;provide a **request** message to the remote server to perform **the** indicated service;receive a response message from the remote server, the response message being affiliated with the **request** message; andrespond to the local **client** device with **information** indicative of the response message; andthe remote **server** able to communicatively couple to the local server and to a remote **client** device that is local to the remote server, the remote server operative to:receive the **request** message from the local server;perform further processing based on the **request** message; andprovide the response **message** to the local server;so that the local **client** device can **request** services **that** are provided by the remote **client** device by using the local and remote servers as intermediaries.

19/3,K/4 (Item 4 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0012941318 *Drawing available*
WPI Acc no: 2003-017991/200301
XRPX Acc No: N2003-013866
**Networked computing apparatus e.g. Web TV for e-commerce business transaction, has HTTP client connected to network interface of inactive server, for transmitting business message to another computing apparatus**
Patent Assignee: BINDER G C (BIND-I); INTEL CORP (ITLC)
Inventor: BINDER G C

Patent Family ( 2 patents, 1 countries )

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---|---|---|---|---|---|---|---|
| US 20020138553 | A1 | 20020926 | US 2001815497 | A | 20010322 | 200301 | B |
| US 7096262 | B2 | 20060822 | US 2001815497 | A | 20010322 | 200656 | E |

Priority Applications (no., kind, date): US 2001815497 A 20010322

Patent Details

| Patent Number | Kind | Lan | Pgs | Draw | Filing Notes |
|---|---|---|---|---|---|
| US 20020138553 | A1 | EN | 21 | 14 | |

**Alerting Abstract** ...NOVELTY - A **HTTP client** coupled to a network interface of an inactive **HTTP** server, transmits a business message to a **HTTP server** of **another**

networked computing apparatus, through a hub. A processor coupled to the **HTTP client** retains the message until a polling **HTTP** POST message is received from the other computing apparatus.

**Original Abstracts:**being coupled to an always-active listening component; and a processing component coupled to the sender component to process a business message or a polling **request** for transfer to **another** networked computing apparatus is disclosed... ... computing apparatus having a business message sender component coupled to a network interface, the network interface not being coupled to an always-active listening component; **and** a **processing** component coupled to the sender component to process a business message or a polling **request** for transfer to another networked computing apparatus is **disclosed.**

**...Claims:**comprising: a business message sender component coupled to a network interface, the network interface not being coupled to an always-active listening component; and a processing component coupled to the sender component to process a business message 5 or a polling request for transfer to another networked computing apparatus. ... ... to a server, the business message having additional data attached;receiving a response from the server confirming the business message was received;sending a polling request to the server;receiving a second response from the server confirming the polling request was received, the second response further including a first receipt acknowledgement of a result of processing the business message and indicating a message queue associated with the server is not empty;sending a second polling request to the server in response to the indication the message queue is not empty;receiving a third response from the server including a second business message including the result of processing the business message, the third response indicating the message queue is empty;storing the second business message; andsending a second receipt acknowledgement including a result of processing the second business message to the server.

19/3,K/5 (Item 5 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0012668212 *Drawing available*
WPI Acc no: 2002-518243/200255
Related WPI Acc No: 2004-707109
XRPX Acc No: N2002-410132
**Communication system has upstream proxy server retrieving HTML content specifying object from web server and forwarding information associated with object to downstream proxy server communicating with client**
Patent Assignee: BORDER J (BORD-I); BUTEHORN M (BUTE-I); DILLON D (DILL-I); HUGHES ELECTRONICS CORP (HUGA)
Inventor: BORDER J; BUTEHORN M; DILLON D

Patent Family ( 4 patents, 27 countries )

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---|---|---|---|---|---|---|---|
| US 20020055966 | A1 | 20020509 | US 2000708134 | A | 20001108 | 200255 | B |
| | | | US 2001996445 | A | 20011128 | | |
| EP 1206100 | A1 | 20020515 | EP 2001309437 | A | 20011107 | 200255 | E |
| BR 200105118 | A | 20040810 | BR 20015118 | A | 20011107 | 200455 | E |
| EP 1206100 | B1 | 20051005 | EP 2001309437 | A | 20011107 | 200569 | E |

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

Priority Applications (no., kind, date): US 2000708134 A 20001108; US 2001996445 A 20011128

Patent Details

| Patent Number | Kind | Lan | Pgs | Draw | Filing Notes | |
|---|---|---|---|---|---|---|
| US 20020055966 | A1 | EN | 19 | 9 | C-I-P of application | US 2000708134 |
| EP 1206100 | A1 | EN | | | | |
| Regional Designated States,Original | AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR | | | | | |
| BR 200105118 | A | PT | | | | |
| EP 1206100 | B1 | EN | | | | |
| Regional Designated States,Original | GB | | | | | |

**Alerting Abstract** ...NOVELTY - An upstream proxy server (107) retrieves **HTML** content specifying object from a web server (109) based on **request** from a **client** and forwards information associated with the object to a downstream proxy server (105) through data network such as WAN, before receiving another **request** from the **client**. The downstream proxy server transmits received information to the **client**. ...

**Original Abstracts:**A communication system for retrieving web content is disclosed. A downstream proxy server (105) receives a URL **request** message from a **web** browser (103), in which the URL **request** message specifies a **URL** content that has an embedded object. An upstream proxy server (107) receives the URL **request** message from the **downstream** proxy server. The upstream proxy server selectively forwards the URL **request** message to a **web** server (109) and receives the URL content from the web server, wherein the upstream proxy server forwards the URL content to the downstream proxy server and parses the URL content to obtain the embedded object prior to receiving a corresponding embedded object **request** message initiated by **the** web browser... ... A communication system for retrieving content stored in a content server (e.g., web server) is disclosed. The system includes a **client** that is configured to transmit a message **requesting content** specifying an object from a content server. **The** system also includes a plurality of proxy servers that include a downstream proxy server and an upstream proxy server. The downstream proxy server is configured to communicate with the **client**. The upstream proxy server is configured to retrieve **the** content from the content server and to forward information associated with the object over a data network to the downstream proxy server prior to **the** client transmitting **another** message **requesting the** object. The above **arrangement** has particular **application to** a wide area network, such as a **satellite** network.

**Claims:**A communication system for retrieving web content, comprising:a downstream proxy server configured to receive a URL **request** message from a **web** browser, the URL **request** message specifying a **URL** content having an embedded object; andan upstream proxy server configured to communicate with the downstream proxy server and to receive the URL **request** message from the downstream proxy **server**, the upstream proxy server selectively forwarding the URL **request** message to a web server **and** receiving the URL content from the web server, wherein the upstream proxy server forwards the URL content to the downstream proxy server and parses the URL content to obtain the embedded object prior to receiving a corresponding embedded object **request** message initiated by the web **browser**.... ... zum Abrufen eines Inhalts, mit:einem ersten Server (107), der an eine

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

Kommunikationsleitung (111) gekoppelt ist und der konfiguriert ist, um eine Nachricht von einen **Client** zu empfangen, der den Inhalt anfordert; undeinem zweiten Server (105), der an **die** Kommunikationsverbindung (111) gekoppelt ist und der konfiguriert ist, um einen Teil des Inhalts an den ersten Server (107) weiterzuleiten, bevor eine weitere Nachricht empfangen wird... ... A communication system (100) for retrieving content, comprising:a **first server** (107) coupled to a communications link (111) and configured to receive a message from a **client requesting** the content; anda **second server** (105) **coupled to** the communications link (111) and configured to forward a portion of the content to the **first server** (107) prior to receiving **another** message **requesting the** portion of the content according to prescribed criteria, **characterised in that** the prescribed criteria include at least one **of a** criterion relating to the sizes of **a** plurality of objects within the content and a criterion relating to capability of the plurality of the objects to be cached... ... Systeme (100) de communication pour recuperer un contenu, comportant:un premier serveur (107) couple a une liaison (111) de communications et **configure** pour recevoir **un** message depuis un **client** demandant le contenu; etun second serveur (105) couple a la liaison (111) **de** communications et **configure** pour **envoyer** une partie du contenu au premier serveur (107) avant la reception **d'un** autre **message** demandant la partie **du** contenu selon des criteres prescrits, **caracterise en ce que** les criteres prescrits comprennent au moins l'**un** d'**un** critere concernant les tailles d'une pluralite d'objets dans le contenu et d'un critere concernant l'aptitude de la pluralite des objets a... ... What is claimed is:**1**. A communication system comprising:a **client** configured to transmit a message **requesting** content specifying an object from a content server; anda plurality of proxy servers including a downstream proxy server and an upstream proxy server, the downstream proxy server being configured to communicate with the **client**,wherein the upstream proxy server is configured to retrieve the content from the content server **and** to forward **information** associated with **the** object over a **data** network to the downstream proxy server prior to the **client transmitting another** message **requesting** the object.

19/3,K/7 (Item 7 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0012302828 *Drawing available*
WPI Acc no: 2002-244174/200230
XRPX Acc No: N2002-188999
**Computer system connected to virtual private network, selects new gateway server upon detection of failure of previously selected gateway, and sets up encrypted communication between selected gateway and client**
Patent Assignee: FUJITSU SERVICES LTD (FUJI-N); INT COMPUTERS LTD (INCM); JAROSZ M J S (JARO-I)
Inventor: JAROSZ M J S

Patent Family ( 8 patents, 27 countries )

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---|---|---|---|---|---|---|---|
| GB 2363548 | A | 20011219 | GB 200014523 | A | 20000615 | 200230 | B |
| EP 1175061 | A2 | 20020123 | EP 2001304169 | A | 20010509 | 200230 | E |
| US 20010054158 | A1 | 20011220 | US 2001862860 | A | 20010522 | 200230 | E |
| EP 1175061 | B1 | 20050216 | EP 2001304169 | A | 20010509 | 200513 | E |
| DE 60108927 | E | 20050324 | DE 60108927 | A | 20010509 | 200523 | E |
| | | | EP 2001304169 | A | 20010509 | | |

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| DE 60108927 | T2 | 20051229 | DE 60108927 | A | 20010509 | 200606 | E |
| | | | EP 2001304169 | A | 20010509 | | |
| US 7000121 | B2 | 20060214 | US 2001862860 | A | 20010522 | 200615 | E |
| DE 60108927 | T8 | 20060504 | DE 60108927 | A | 20010509 | 200632 | E |
| | | | EP 2001304169 | A | 20010509 | | |

Priority Applications (no., kind, date): GB 200014523 A 20000615

Patent Details

| Patent Number | Kind | Lan | Pgs | Draw | Filing Notes | |
|---|---|---|---|---|---|---|
| GB 2363548 | A | EN | 17 | 2 | | |
| EP 1175061 | A2 | EN | | | | |
| Regional Designated States,Original | AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR | | | | | |
| EP 1175061 | B1 | EN | | | | |
| Regional Designated States,Original | DE FR GB | | | | | |
| DE 60108927 | E | DE | | | Application | EP 2001304169 |
| | | | | | Based on OPI patent | EP 1175061 |
| DE 60108927 | T2 | DE | | | Application | EP 2001304169 |
| | | | | | Based on OPI patent | EP 1175061 |
| DE 60108927 | T8 | DE | | | Application | EP 2001304169 |
| | | | | | Based on OPI patent | EP 1175061 |

**Alerting Abstract** ...NOVELTY - A **client** node (1) is connected to the target nodes (5-7) through gateway servers (21-23). A key management service (8) selects a gateway server and sets up encrypted communication between the selected gateway and the **client**. A new gateway is selected, when the failure of previously selected gateway is detected, and accordingly the encrypted communication is set up between the new gateway and the **client**. ...USE - Computer system including **client** nodes connected to LAN through virtual private network including a link such as Internet or direct remote access service (RAS) dial-in connection... ...unsuccessful communication due to partial or full failure of a gateway server, is prevented by selecting new gateway and setting up encrypted communication between the **client** and the gateway... ...

**Original Abstracts:**A first node (**client**) (1) is in **communication** with one of a plurality of second nodes (5, 6, 7) connected to a local area network (LAN) (4) via a virtual private network including a link (3), such as the Internet, and a selected one of a plurality of third nodes (gateway servers) (21, 22, 23). **Communication** between the **first** node (1) and the third nodes (21, 22, 23) is encrypted, whereas communication between the third nodes and the second nodes (5, 6, 7) is... ... A first node (**client**) (**1**) is in communication with one of a **plurality** of second nodes (**5, 6, 7**) connected to a local area network (LAN) (**4**) via a virtual private network including a link (**3**), such as... ... A first node (**client**) (**1**) is in communication with one of a plurality of second nodes (**5, 6, 7**) connected to a local area network (LAN) (**4**) via a virtual private network including a link (**3**), such as the **Internet**, and a selected one of a plurality of third nodes (**gateway servers**) (**21, 22, 23**). Communication between the first node (**1**) and the third nodes (**21, 22, 23**) is encrypted,

whereas communication between the third nodes and the second nodes (**5, 6, 7**) is unencrypted. Communication from the first node (**1**) to one of **the second** nodes (**5, 6, 7**) is initially set up via a selected one of the third nodes after suitable authentication. If that third node should subsequently...
...**Claims:**8) for selecting the third node comprises a key management service which selects a third node from the plurality and attempts to perform a said **authentication** process **therewith** upon a **request** by **the** first node for a said message encryption key, and wherein upon successful authentication the said message encryption key is generated and cached at the first... ... 8) for selecting the third node comprises a key management service which selects a third node from the plurality and attempts to perform said respective **authentication** process therewith upon a **request** by the first node **for** a said respective message **encryption** key, and wherein upon successful authentication said first node (1) and the selected third node (21, 22, 23)cache said respective message encryption key... des communications entre le premier noeud et chacun des troisiemes noeuds sont cryptees via une cle de cryptage de message respective qui est etablie apres **un processus** d'authentification respectif, ou le moyen (8) pour selectionner le troisieme noeud **comprend un** service de gestion de cle qui selectionne un troisieme noeud parmi la pluralite et qui tente de realiser ledit **processus** d'**authentification** respectif en relation avec suite a une requete au moyen du premier noeud pour une dite cle de cryptage de message respective et ou, suite... ... means for selecting the third node comprises a key management service which selects a third node from the plurality and attempts to perform a said **authentication** process therewith upon a **request** by the first node for a said message encryption key, and wherein upon successful **authentication** the said message encryption **key** is generated and cached at the first node and the selected third node... ... which is held in a cache store in the first node to encrypt communications between the first node and said one of the gateway nodes;(**b**) the **first** node monitors said one of the gateway nodes for failure;(c) in the event of failure of said one **of** the **gateway** nodes, the **first** node **deletes** the session key from the cache store and searches the cache store **to** determine whether **another** session key has been cached allowing a new VPN connection to be established **with** the **second node** by way of **another** of the **gateway** nodes;(d) in the event that another session key has not been cached, the first node initiates a key establishment **protocol** exchange with a selected one **of** the **gateway** nodes, **other than** the failed **node**, to establish a new session key allowing a new VPN connection to be established with the second node by way of said **selected** one of the gateway nodes, the new **session** key **being** saved in the cache store.

19/3,K/14 (Item 14 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0009697757 *Drawing available*
WPI Acc no: 1999-337568/199928
**Operations authorizing determining in stateless web environment**
Patent Assignee: ORACLE CORP (ORAC); ORACLE INT CORP (ORAC)
Inventor: PANG R; STABILE J

Patent Family ( 11 patents, 8 countries )

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---|---|---|---|---|---|---|---|
| WO 1999023786 | A2 | 19990514 | WO 1998US22832 | A | 19981029 | 199928 | B |
| AU 199912035 | A | 19990524 | AU 199912035 | A | 19981029 | 199940 | E |
| EP 1027795 | A2 | 20000816 | EP 1998955165 | A | 19981029 | 200040 | E |
| | | | WO 1998US22832 | A | 19981029 | | |

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| JP 2001522115 | W | 20011113 | WO 1998US22832 | A | 19981029 | 200204 | E |
| | | | JP 2000519525 | A | 19981029 | | |
| AU 750435 | B | 20020718 | AU 199912035 | A | 19981029 | 200258 | E |
| US 6446204 | B1 | 20020903 | US 1997961796 | A | 19971031 | 200260 | E |
| EP 1027795 | B1 | 20040107 | EP 1998955165 | A | 19981029 | 200405 | E |
| | | | WO 1998US22832 | A | 19981029 | | |
| DE 69821020 | E | 20040212 | DE 69821020 | A | 19981029 | 200419 | E |
| | | | EP 1998955165 | A | 19981029 | | |
| | | | WO 1998US22832 | A | 19981029 | | |
| EP 1027795 | B9 | 20040908 | EP 1998955165 | A | 19981029 | 200459 | E |
| | | | WO 1998US22832 | A | 19981029 | | |
| JP 3853593 | B2 | 20061206 | WO 1998US22832 | A | 19981029 | 200680 | E |
| | | | JP 2000519525 | A | 19981029 | | |
| CA 2308797 | C | 20080325 | CA 2308797 | A | 19981029 | 200824 | E |
| | | | WO 1998US22832 | A | 19981029 | | |

Priority Applications (no., kind, date): US 1997961796 A 19971031

Patent Details

| Patent Number | Kind | Lan | Pgs | Draw | Filing Notes | |
|---|---|---|---|---|---|---|
| WO 1999023786 | A2 | EN | 59 | 8 | | |
| AU 199912035 | A | EN | | | Based on OPI patent | WO 1999023786 |
| EP 1027795 | A2 | EN | | | PCT Application | WO 1998US22832 |
| | | | | | Based on OPI patent | WO 1999023786 |
| Regional Designated States,Original | DE FR GB NL | | | | | |
| JP 2001522115 | W | JA | 84 | | PCT Application | WO 1998US22832 |
| | | | | | Based on OPI patent | WO 1999023786 |
| AU 750435 | B | EN | | | Previously issued patent | AU 9912035 |
| | | | | | Based on OPI patent | WO 1999023786 |
| EP 1027795 | B1 | EN | | | PCT Application | WO 1998US22832 |
| | | | | | Based on OPI patent | WO 1999023786 |
| Regional Designated States,Original | DE FR GB NL | | | | | |
| DE 69821020 | E | DE | | | Application | EP 1998955165 |
| | | | | | PCT Application | WO 1998US22832 |
| | | | | | Based on OPI patent | EP 1027795 |
| | | | | | Based on OPI patent | WO 1999023786 |
| EP 1027795 | B9 | EN | | | PCT Application | WO 1998US22832 |
| | | | | | Based on OPI patent | WO 1999023786 |
| Regional Designated | DE FR GB NL | | | | | |

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

| States,Original | | | | | | |
|---|---|---|---|---|---|---|
| JP 3853593 | B2 | JA | 37 | | PCT Application | WO 1998US22832 |
| | | | | | Previously issued patent | JP 2001522115 |
| | | | | | Based on OPI patent | WO 1999023786 |
| CA 2308797 | C | EN | | | PCT Application | WO 1998US22832 |
| | | | | | Based on OPI patent | WO 1999023786 |

**Alerting Abstract** ...configured to process database queries according to the Oracle-based Programming Language using Structured Query Language (PL/SQL). The PL/SQL runtime executes a browser **request** having a database query. For example, assume that a listener (210) receives a browser **request** over the Internet (208) delivered in the form of a Uniform Resource Locator (URL). The browser **request** serves as an identifier for a web object, for example an **HTML** page or an operation to be performed.

**Original Abstracts:**A highly scalable, flexible, and extensible mechanism is provided for authenticating a **request** from a **client**. In a preferred embodiment, the invention comprises an authentication engine, an authentication host, a plurality of providers coupled to the host which implement selected authentification... ... machine each component resides on. The communication mechanism enables the invention to be distributed, which in turn, makes the invention highly scalable. In operation, the **authentication** engine receives a **request** having associated therewith a protect string. The protect string specifies the **authentication** scheme or schemes that **need** to be implemented for that **request**.The **authentication** engine parses the protect string into one or more provider **requests**, and sends the **requests** to the **authentication** host. In response, the host forwards the **requests** to the appropriate providers for processing. The results of the providers' processing are sent back to the authentication engine, which then processes the results according to the protect string to determine whether the **request** has been authenticated. With the present invention, it is possible to add providers to the system, or to substitute a new provider for an existing provider, without changing or recompiling any **other component** in the system. It is also possible to change the **authentication** schemes associated with a **request** by simply changing the protect string. These aspects of the invention make it possible to change implementation at deployment time, as opposed to compile time... ... A highly scalable, flexible, and extensible mechanism is provided for authenticating a **request** from a **client**. In a preferred embodiment, the invention comprises an authentication engine, an authentication host, a plurality of providers coupled to the host which implement selected authentication... ... machine each component resides on. The communication mechanism enables the invention to be distributed, which in turn, makes the invention highly scalable. In operation, the **authentication** engine receives a **request** having associated therewith a protect string. The protect string specifies the **authentication** scheme or schemes that **need** to be implemented for that **request**. The **authentication** engine parses the protect string into one or more provider **requests**, and sends the **requests** to the **authentication** host. In response, the host forwards the **requests** to the appropriate providers for processing. The results of the providersprime processing are sent back to the authentication engine, which then processes the results according to the protect string to determine whether the **request** has been authenticated. With the present invention, it is possible to add providers to the system, or to substitute a new provider for an existing provider, without changing or recompiling any **other component** in the system. It is also possible to change the **authentication** schemes associated with a **request** by simply changing the protect string. These aspects of the invention make it possible to change implementation at deployment time, as opposed to compile time... ... A highly scalable, flexible, and extensible mechanism is provided for

authenticating a **request** from a **client**. In a preferred embodiment, the invention comprises an authentication engine, an authentication host, a plurality of providers coupled to the host which implement selected authentification... ... machine each component resides on. The communication mechanism enables the invention to be distributed, which in turn, makes the invention highly scalable. In operation, the **authentication** engine receives a **request** having associated therewith a protect string. The protect string specifies the **authentication** scheme or schemes that **need** to be implemented for that **request**.The **authentication** engine parses the protect string into one or more provider **requests**, and sends the **requests** to the **authentication** host. In response, the host forwards the **requests** to the appropriate providers for processing. The results of the providers' processing are sent back to the authentication engine, which then processes the results according to the protect string to determine whether the **request** has been authenticated. With the present invention, it is possible to add providers to the system, or to substitute a new provider for an existing provider, without changing or recompiling any **other component** in the system. It is also possible to change the **authentication** schemes associated with a **request** by simply changing the protect string. These aspects of the invention make it possible to change implementation at deployment time, as opposed to compile time... ... L'invention concerne un mecanisme extensible, hautement reglable et flexible, destine a authentifier une demande emanant d'un **client**. Dans un mode de realisation prefere, l'invention comprend un moteur d'authentification, un hote d'authentification, plusieurs fournisseurs couples a l'hote et mettant...

...**Claims:** Said 1st message is an implication about the permission information link|related with cartridge (230) including the step which transmits a 1st message to a certification|authentication server (252) from dispatcher (214) transparent with respect to said **client** and said cartridge.Further,A 2nd message with respect to said **client** and said cartridge transparentIt is shown whether including the step which transmits to dispatcher (214) from a certification|authentication **server** (252), said **2nd** message is permitted so that operation may be performed by cartridge (230).Further,When it permits so that operation may be performed by cartridge (230... a first machine, the method comprising the steps of:executing a dispatcher on a second machine, wherein the dispatcher is a component configured to receive **requests** for multiple destinations and to route each of said multiple **requests** to one or more of said multiple destinations; wherein said multiple destinations include said cartridge and one or more destinations other than said cartridge;executing at least one component of an authentication server on a third machine;receiving a **request** at said dispatcher from a **client** executing on a machine that is different from said second machine;sending a first message, transparent to said **client** and said cartridge, from the dispatcher to the authentication **server**, wherein the **first** message contains authorization information that is associated with the cartridge;sending a second message, transparent to said **client** and said cartridge, from the authentication server to the dispatcher, wherein the second message indicates whether the operation is authorized to be performed by the...

19/3,K/17 (Item 17 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0008866683 *Drawing available*
WPI Acc no: 1998-414290/199835
XRPX Acc No: N1998-322405
**Data access control for Internet server - Replaces reference with token for comparison of tokens and client identities to generate HTML-formatted document**

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

**with URLs**

Patent Assignee: BRITISH TELECOM PLC (BRTE)

Inventor: MCGEE N G

Patent Family ( 7 patents, 78 countries )

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---|---|---|---|---|---|---|---|
| WO 1998032066 | A1 | 19980723 | WO 1998GB53 | A | 19980109 | 199835 | B |
| AU 199854924 | A | 19980807 | AU 199854924 | A | 19980109 | 199901 | E |
| EP 953170 | A2 | 19991103 | EP 1998900317 | A | 19980109 | 199951 | E |
| | | | WO 1998GB53 | A | 19980109 | | |
| JP 2001508901 | W | 20010703 | JP 1998533916 | A | 19980109 | 200142 | E |
| | | | WO 1998GB53 | A | 19980109 | | |
| US 6393468 | B1 | 20020521 | WO 1998GB53 | A | 19980109 | 200239 | E |
| | | | US 199843146 | A | 19980313 | | |
| EP 953170 | B1 | 20030910 | EP 1998900317 | A | 19980109 | 200360 | E |
| | | | WO 1998GB53 | A | 19980109 | | |
| DE 69818008 | E | 20031016 | DE 69818008 | A | 19980109 | 200376 | E |
| | | | EP 1998900317 | A | 19980109 | | |
| | | | WO 1998GB53 | A | 19980109 | | |

Priority Applications (no., kind, date): EP 1997300331 A 19970120

Patent Details

| Patent Number | Kind | Lan | Pgs | Draw | Filing Notes | |
|---|---|---|---|---|---|---|
| WO 1998032066 | A1 | EN | 30 | 8 | | |
| National Designated States,Original | AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW | | | | | |
| Regional Designated States,Original | AT BE CH DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW | | | | | |
| AU 199854924 | A | EN | | | Based on OPI patent | WO 1998032066 |
| EP 953170 | A2 | EN | | | PCT Application | WO 1998GB53 |
| | | | | | Based on OPI patent | WO 1998032066 |
| Regional Designated States,Original | DE FR GB | | | | | |
| JP 2001508901 | W | JA | 38 | | PCT Application | WO 1998GB53 |
| | | | | | Based on OPI patent | WO 1998032066 |
| US 6393468 | B1 | EN | | | PCT Application | WO 1998GB53 |
| | | | | | Based on OPI patent | WO 1998032066 |
| EP 953170 | B1 | EN | | | PCT Application | WO 1998GB53 |
| | | | | | Based on OPI patent | WO 1998032066 |

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

| | | | | | | |
|---|---|---|---|---|---|---|
| Regional Designated States,Original | DE FR GB | | | | | |
| DE 69818008 | E | DE | | | Application | EP 1998900317 |
| | | | | | PCT Application | WO 1998GB53 |
| | | | | | Based on OPI patent | EP 953170 |
| | | | | | Based on OPI patent | WO 1998032066 |

**Alerting Abstract** ...The device includes a session manager for receiving a **request** from a **client** for an item of information which has at least one reference to a further item of information. The item is modified by replacing the reference with a token, the token and reference are stored and the modified item of information is returned to the **client**. ... ...The server used has a random number generator and stores the **client** identity in association with each token and its reference... ...ADVANTAGE - Provides tailored interface to service provider database using conventional Web browser and Internet connection. Obviates **need** to transfer **information** from existing database onto Web server and customer login password records remain in database, which is separate from Internet server. This improves security and reduces

**Original Abstracts:**A modified Web server (310) comprises a session manager (320) which intercepts all incoming **requests** from **clients** for **Web** pages. **Each request** incorporates a token **which** the session manager (320) compares with tokens which are stored in a session store (330). Once finding a matching token, a URL associated with the matching token is used by the Web server (310) to return a Web page indicated by the URL to the **requester**. Any URLs embedded **in** the Web page to be returned are tokenised by the session manager (320) before the page is returned, and the resulting token/URL pair is... ... A modified Web server comprises a session manager which intercepts all incoming **requests** from **clients** for Web **pages**. Each **request** incorporates a token which **the** session manager compares with tokens which are stored in a session store. On finding a matching token, a URL associated with the matching token is used by the Web server to return a Web page indicated by the URL to the **requester**. Any URLs embedded in **the** Web page to be returned are tokenised by the session manager before the page is returned, and the resulting token/URL pair is stored in... ... A modified Web server (310) comprises a session manager (320) which intercepts all incoming **requests** from **clients** for Web pages. Each **request** incorporates **a** token **which** the session manager (320) **compares** with tokens which are stored in a session store (330). Once finding a matching token, a URL associated with the matching token is used by the Web server (310) to return a Web page indicated by the URL to the **requester**. Any URLs embedded in the Web page to **be** returned are tokenised by the session manager (320) before the page is returned, and the resulting token/URL pair is stored in the session store... ...**Claims:**An information server (300) having:means (310) for receiving a **request** from a **client** for an item of information, said item of information including at least one reference **to** a further **item** of **information**;means (320) configured to replace the or each reference by a token, thereby modifying the item of information;storage means (330) to store the or each token and the or each respective reference;means (310) configured to return to the **client** the modified item of information.Serveur d'informations (300) comportant:un moyen (310) destine a recevoir une demande d'un **client** pour un element d'informations, ledit element d'informations comprenant au moins une reference vers un autre element d'informations,**un moyen** (320) **configure** pour remplacer la ou chaque reference par **un** jeton, modifiant ainsi l'element d'informations,un moyen de memorisation (330) destine a memoriser le ou chaque jeton et la ou **chaque** reference respective,**un** moyen (310) **configure** pour

renvoyer au **client** l'element d'informations modifie.An information server comprising:means for establishing a session between a **client** and an information server;means for receiving at said **information server** a **first request** from the **client** for an item of information, said item of information including a plurality of references to a plurality of further items of information;means for modifying the item of **information** by replacing at least one reference by a token;means for **storing data** that **relates each** token to **its** corresponding reference in storage means for the duration of said session;means for returning to the **client** the modified item of information in which at least one reference has been replaced by a token;means for receiving at said **information server** a **second request** from **the client** for an item of **information**, the second **request** including a token indicative of the item of **information requested**;means for comparing the token **with** the tokens which have been stored in said storage means during said session to find a matching stored token; andmeans for returning to **the client**, in **dependence upon** finding a **matching** stored token, the respective **corresponding** item of **information.**

19/3,K/20 (Item 20 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0007104379 *Drawing available*
WPI Acc no: 1995-132972/199518
XRPX Acc No: N1995-104654
**Usage management for access data on telecommunications network - using dial-up line between remote central service and local subscriber allowing interaction through managing module in order to control usage**
Patent Assignee: FRANCE TELECOM (ETFR); TELEDIFFUSION DE FRANCE (TELG); TELEDIFFUSION DE FRANCE SA (TELG)
Inventor: LECLERCQ T; SALLIO P

Patent Family ( 6 patents, 7 countries )

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---|---|---|---|---|---|---|---|
| EP 647052 | A1 | 19950405 | EP 1994402194 | A | 19940930 | 199518 | B |
| FR 2711026 | A1 | 19950414 | FR 199311801 | A | 19931004 | 199520 | E |
| JP 7183885 | A | 19950721 | JP 1994240401 | A | 19941004 | 199538 | E |
| US 5696902 | A | 19971209 | US 1994316466 | A | 19941003 | 199804 | E |
| EP 647052 | B1 | 20030319 | EP 1994402194 | A | 19940930 | 200325 | E |
| DE 69432280 | E | 20030424 | DE 69432280 | A | 19940930 | 200335 | E |
| | | | EP 1994402194 | A | 19940930 | | |

Priority Applications (no., kind, date): FR 199311801 A 19931004; EP 1994402194 A 19940930

Patent Details

| Patent Number | Kind | Lan | Pgs | Draw | Filing Notes |
|---|---|---|---|---|---|
| EP 647052 | A1 | FR | 16 | 4 | |
| Regional Designated States,Original | DE GB IT SE | | | | |
| JP 7183885 | A | JA | 13 | | |

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

| | | | | | | |
|---|---|---|---|---|---|---|
| US 5696902 | A | EN | 15 | | | |
| EP 647052 | B1 | FR | | | | |
| Regional Designated States,Original | DE GB IT SE | | | | | |
| DE 69432280 | E | DE | | | Application | EP 1994402194 |
| | | | | | Based on OPI patent | EP 647052 |

**Alerting Abstract** ...The **protocol** has several stages. The terminal is connected to the module and the connection discharged. An authorisation message **requesting** service is sent by the module to the central server on half of the terminals. On validation by the server, a connection **request** is sent by the terminal to the server. After validation by the server, data is transmitted and exchanged between the terminal and the server for the service **requested**. Following provision of the service, the central server transmits to the module a message to account for the service provided...
**Original Abstracts:**MG) for the charging is provided, this module being external to the link and making it possible, by interactive communication between the local subscriber terminal (**T**) and **the management** module (**MG**), as well as between the management module (MG) and the remote server centre (SA), to establish, monitor and bill for the query between the remote server centre (SA) and a subscriber terminal (**T**). **Application to managing queries** from **server** centres on national or international networks...

...**Claims:**an interactive type between said local subscriber terminal and said management means and between said management means and said remote server center, respectively, a communication **protocol** including successive steps comprising: connection of said local subscriber terminal to said management means, acknowledgement of said connection and issuing of an **access key** providing **access** to **said** remote **server** center, transmission by said management means to said remote server center of a service **request authorization** message with respect to **a corresponding** subscriber **terminal**, and, on a **first** validation, by said remote server center, of said service **request authorization** message, **request** for connection and **service provision** of said local subscriber terminal to said remote **server** center, by **transmission** to said remote server center of a connection **request message comprising** said **access key**, **and** on a second validation of said connection **request** message, transmission of **data** between said remote server center and said local subscriber terminal in accordance with **said requested** service provision, **and subsequent** to said **requested** service provision being supplied and, **transmission** by said remote server center to said management means of a status message indicating the status of said **requested** service **provision.**

**~~ Patent Literature Full-Text**

15/3K/5 (Item 3 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT

00853825

**SYSTEMS, METHODS AND COMPUTER PROGRAM PRODUCTS FOR DYNAMICALLY INSERTING CONTENT INTO WEB DOCUMENTS FOR DISPLAY BY CLIENT DEVICES**
SYSTEMES, PROCEDES ET PRODUITS DE PROGRAMMES INFORMATIQUES DESTINES A INSERER DYNAMIQUEMENT DU CONTENU DANS DES DOCUMENTS WEB DESTINES A ETRE AFFICHES PAR DES DISPOSITIFS CLIENTS

**Patent Applicant/ Patent Assignee:**

- **WINDWIRE INC**
  100 Perimeter Park Drive, Suite I, Morrisville, NC 27560; US; US(Residence); US(Nationality); (For all designated states except: US)

**Patent Applicant/ Inventor:**

- **BORGER Dana**
  130 Loch Lomond Circle, Cary, NC 27511; US; US(Residence); US(Nationality); (Designated only for: US)
- **COX Steve**
  2506 Lake Elton Road, Durham, NC 27713; US; US(Residence); US(Nationality); (Designated only for: US)
- **GORDON Tom**
  363 East 76 Street, Apt. 19A, New York, NY 10021; US; US(Residence); US(Nationality); (Designated only for: US)
- **SPITZ David**
  5320 Deergrass Court, Raleigh, NC 27613; US; US(Residence); US(Nationality); (Designated only for: US)
- **SQUIRE Matthew**
  10105 Touchwood Place, Raleigh, NC 27613; US; US(Residence); US(Nationality); (Designated only for: US)
- **THRASH Jay**
  303 Trappers Run Drive, Cary, NC 27513; US; US(Residence); US(Nationality); (Designated only for: US)

**Legal Representative:**

- **MYERS BIGEL SIBLEY & SAJOVEC(agent)**
  P.O. Box 37428, Raleigh, NC 27627; US;

| | Country | Number | Kind | Date |
|---|---|---|---|---|
| Patent | WO | 200186544 | A2 | 20011115 |
| Application | WO | 2001US13681 | | 20010430 |
| Priorities | US | 2000202774 | | 20000509 |

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

| | Country | Number | Kind | Date |
|---|---|---|---|---|
| | US | 2000220559 | | 20000725 |
| | US | 2001799194 | | 20010305 |

**Designated States:** (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG,
BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE,
GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU,
LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO,
NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK,
SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ,
VN, YU, ZA, ZW

**[EP]** AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LU; MC; NL; PT; SE; TR;

**[OA]** BF; BJ; CF; CG; CI; CM; GA; GN; GW; ML;
MR; NE; SN; TD; TG;

**[AP]** GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;
UG; ZW;

**[EA]** AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

**Language** Publication Language: English
Filing Language: English
Fulltext word count: 9017

**Detailed Description:**

...for including advertisements within
content), and an advertiser has another ad serving
solution. In such situations, the normal operation is as
follows. The publisher ad **server** receives an **initial** ad
request from a user1s browser and selects an
advertisement. This advertisement may in fact be a
reference (URL) to another ad server (possibly owned mark)reless client
device to a **first server** (e.g., a Web server), via a
communications network (e.g., the Internet, an intranet,
etc.). In response to receiving the user request, the
**first server** sends a request to a **second server** (e.g., a
third party ad **server**) for **additional** content (e.g., an
advertisement, such as an image and/or text) to be
included within the requested Web document. The location
of the additional... ...markup tags. Additional information, such as
format of the content, may be specified by the markup
tags as well.

The content request sent to the **second server**

may include any information that was received by the first server with the user request including, but not limited to, user information and content format **information**. A user request may include information contained within a cookie stored within a user,s wireless client device. In addition, a user **request** may include **information** contained within HTTP headers associated with the user request. The **second server** may select content for inclusion within the Web document based upon user information accompanying the content request.

Content selected by the **second server** for inclusion with the Web document may not have the format specified by the markup tags within the Web document.

According to embodiments of the present invention, the **second server** may be configured to transcode the content to the format specified by the markup tags. The **second server** sends content having a format specified by the markup tags to the **first server**. The **first server** then serves the Web document to the wireless client device with the additional content included therewithin at the identified location.

According to additional embodiments of the present invention, a user sends a request for a Web document from a wireless client device to a **first server**, via a communications network. In response to receiving the user request, the **first server** sends a request to a second **server** for a **first** content portion (e.g., an advertisement, such as an image and/or text) to be included within the requested Web document. The location of the... ...of the first content portion is specified by the first markup tag.

In response to receiving the request for the first content portion, the second **server** selects a **first** content portion having a format specified by the first markup tag. If a first content portion does not have a format specified by the first... ...portion having a format specified by the second markup tag.

The third server then sends the second content portion to the second server. The second **server** sends the **first** content portion with the second content portion included therewithin to the **first server**. The **first server** then serves the Web document to the wireless client device with the first and second content portions included therewithin at the identified location.

15/3K/27 (Item 25 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results


00484627

**INTEGRATED BUSINESS SYSTEM FOR WEB BASED TELECOMMUNICATIONS MANAGEMENT**
SYSTEME D'ECHANGES COMMERCIAUX INTEGRES POUR LA GESTION DE TELECOMMUNICATIONS SUR LE WEB

**Patent Applicant/ Patent Assignee:**

- **BARRY B Reilly**
- **CHODORONEK Mark A**
- **DeROSE Eric**
- **GONZALES Mark N**
- **JAMES Angela R**
- **LEVY Lynne**
- **TUSA Michael**

**Inventor(s):**

- **BARRY B Reilly**
- **CHODORONEK Mark A**
- **DeROSE Eric**
- **GONZALES Mark N**
- **JAMES Angela R**
- **LEVY Lynne**
- **TUSA Michael**

| | Country | Number | Kind | Date |
|---|---|---|---|---|
| Patent | WO | 9915979 | A1 | 19990401 |
| Application | WO | 98US20170 | | 19980925 |
| Priorities | US | 9760655 | | 19970926 |

**Designated States:** (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AU, BR, CA, JP, MX, SG, AT, BE, CH, CY,
DE, DK, ES, FI, FR, GB, GR, IE, IT, LU,
MC, NL, PT, SE

**Language** Publication Language: English

Filing Language:

Fulltext word count: 88075

**Detailed Description:**

...when a customer clicks on the icon
from the gomepage (Figure 4) for a service such as
TFNM.

In addition, as mentioned, when a customer

**first** logs on, the customer is ...Receiver object 2350 as shown in Figure 25(b). Particularly, the SvcInqCSMRequester object 2310 is the class that represents the re@uester which takes the **request data** that comes from t e Front-End/**Client** 'agplication through the Transaction Manager 2320 uilds the CSM/SI request transactions bK interacting with the Translator classes 2380 and s ips off the **requests** to CSM. The **request data** that comes from the Front End/**Client** is an array of strings that are required from the customer for the re uest to be made. Minimal information is passed from Ne client to reduce the communication overhead from the **client** to the SI 4piplication **server**. All **other information** is packaged in the **Requester**. Particularly, the Requester object 2310 uses the SvcInqRegistryHeader and SvcInqSIHeader classes in the Translator 2380 to build the I/ Registry Header" and "SI Header" strings...

19/3K/5 (Item 4 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT

01252577

**AN INTERNET PROTOCOL COMPATIBLE ACCESS AUTHENTICATION SYSTEM**
SYSTEME D'AUTHENTIFICATION D'ACCES COMPATIBLE AVEC UN PROTOCOLE INTERNET

**Patent Applicant/ Patent Assignee:**

- **SIEMENS MEDICAL SOLUTIONS HEALTH SERVICES CORPORATION**
  51 Valley Stream Parkway, Malvern, Pennsylvania 19355; US; US(Residence); US(Nationality); (For all designated states except: US)

**Patent Applicant/ Inventor:**

- **ANUSZEWSKI David**
  1804 Alyssa Lane, Pottstown, Pennsylvania 19465; US; US(Residence); US(Nationality); (Designated only for: US)

**Legal Representative:**

- **BURKE Alexander J(et al)(agent)**
  Siemens Corporation- Intellectual Property Dept., 170 Wood Avenue South, Iselin, New Jersey 08830; US;

| | Country | Number | Kind | Date |
|---|---|---|---|---|
| Patent | WO | 200559728 | A1 | 20050630 |
| Application | WO | 2004US42530 | | 20041217 |

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

| | Country | Number | Kind | Date |
|---|---|---|---|---|
| Priorities | US | 2003530361 | | 20031217 |
| | US | 200413084 | | 20041215 |

**Designated States:** (All protection types applied unless otherwise stated - for applications 2004+)
AE; AG; AL; AM; AT; AU; AZ; BA; BB; BG;
BR; BW; BY; BZ; CA; CH; CN; CO; CR; CU;
CZ; DE; DK; DM; DZ; EC; EE; EG; ES; FI;
GB; GD; GE; GH; GM; HR; HU; ID; IL; IN;
IS; JP; KE; KG; KP; KR; KZ; LC; LK; LR;
LS; LT; LU; LV; MA; MD; MG; MK; MN; MW;
MX; MZ; NA; NI; NO; NZ; OM; PG; PH; PL;
PT; RO; RU; SC; SD; SE; SG; SK; SL; SY;
TJ; TM; TN; TR; TT; TZ; UA; UG; US; UZ;
VC; VN; YU; ZA; ZM; ZW;

**[EP]** AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;
FI; FR; GB; GR; HU; IE; IS; IT; LT; LU;
MC; NL; PL; PT; RO; SE; SI; SK; TR;

**[OA]** BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;
ML; MR; NE; SN; TD; TG;

**[AP]** BW; GH; GM; KE; LS; MW; MZ; NA; SD; SL;
SZ; TZ; UG; ZM; ZW;

**[EA]** AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

**Language** Publication Language: English
Filing Language: English
Fulltext word count: 7546

**Detailed Description:**

...user, via the client 101, performs a one-time entry of credential information 216 (see FIG. 2), such as a user identifier 219 and a **password** 220, to access to more than one application, or to obtain access to a number of resources within the system 100. Single sign on removes... ...application to another, and allows a task sequence workflow to continue without interruption. The different applications requiring sign on may be implemented on the same **server** or on **different servers**. For example, the user, via the client 101, enters credential **information** a single time to **access** the first application 106 on the **first server** 102 and to access the second application 107 on the **second server** 103.

5
The single sign on process provides at least the following advantages.

1. Allows resources to be secured by HTTP basic authentication.

2. Allows resources to utilize infrastructure that works using HTTP basic **authentication**.

3. Enables **required components**, **other** than an Internet Browser, to be downloaded to

the client 1 0 1 on demand via HTTP requests. ,
4. Does not require separate software to capture credential information.

5. Secures the management and delivery of credentials.

6. Does not require expensive certificate management **processes**/solutions.

7. Does **not** require **HTTP** server side cookies
FIG. 2 illustrates the client 101 and the second server 103 for the system 100, as shown in FIG. 1. The client...

19/3K/6 (Item 5 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT

01022577

**SYSTEM AND METHOD USING LEGACY SERVERS IN RELIABLE SERVER POOLS**
SYSTEME ET PROCEDE COMPRENANT L'UTILISATION DE SERVEURS PATRIMONIAUX DANS DES GROUPEMENTS DE SERVEURS FIABLES

**Patent Applicant/ Patent Assignee:**

- **NOKIA CORPORATION**
  Keilalahdentie 4, FIN-02150 Espoo; FI; FI(Residence); FI(Nationality)
- **NOKIA INC**
  6000 Connection Drive, Irving, TX 75039; US; US(Residence); US(Nationality); (Designated only for: LC)

**Inventor(s):**

- **NARAYANAN Ram Gopal Lakshmi**
  Two Kimball Court, Apt. 506, Woburn, MA 01801; US

**Legal Representative:**

- **WRIGHT Bradley C(agent)**
  Banner & Witcoff, Ltd., 1001 G Street, N.W., Eleventh Floor, Washington, DC 20001-4597; US;

| | Country | Number | Kind | Date |
|---|---|---|---|---|
| Patent | WO | 200352618 | A1 | 20030626 |
| Application | WO | 2002IB5404 | | 20021213 |
| Priorities | US | 200124441 | | 20011218 |

**Designated States:** (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG,
BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD,
GE, GH, GM, HR, HU, ID, IL, IN, IS, JP,
KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT,
LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ,
NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD,
SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ,
UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW

**[EP]** AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;
FI; FR; GB; GR; IE; IT; LU; MC; NL; PT;
SE; SI; SK; TR;

**[OA]** BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;
ML; MR; NE; SN; TD; TG;

**[AP]** GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;
UG; ZM; ZW;

**[EA]** AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

**Language** Publication Language: English
Filing Language: English
Fulltext word count: 3958

**Detailed Description:**

...for example RSerPool physical element 25, and transmits the login request to RSerPool physical element 25 via the data link 59. File transfer protocol control **data** initiates the **requested** file transfer. As can, be appreciated by one ski.lled in the relevant art, RSerPool-unaware client 35 is typically a legacy client which **supports** an application **protocol not supported** by ENRP name server 29. Proxy gateway 37 acts as a relay between ...unaware client 35 enabling the
- 5 combination of RSerPool-unaware client 35 and proxy gateway 37, functioning as an RSerPool client 33, to communicate with **second** name **server** pool 21,
[231 ASAP can be used to exchange auxiliary information between RSerPool-aware client 31 and RSerPool physical element 15 via data link 45... ...and RSerPool physical element 25 via data link 44, before commencing in data transfer. The protocols also allow for RSerPool physical element 17 in the **first** name **server** pool I I to function as an RSerPool client with respect to **second** name **server** pool 21 when RSerPool physical element 17 initiates communication with RSerPool physical element 23 in **second** name **server** pool 21 via a data link 61. Additionally, a data link 63 can be used to fulfill various name space operation, administration, and maintenance (OAM...

19/3K/7 (Item 6 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT

00992401

**SELECTIVE OFFLOADING OF PROTOCOL PROCESSING**
DELESTAGE SELECTIF D'UN TRAITEMENT DE PROTOCOLE

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

**Patent Applicant/ Patent Assignee:**

- **ARCHDUKE DESIGN INC**
  24700 Skyland Road, Los Gatos, CA 95033; US; US(Residence); US(Nationality); (For all designated states except: IS)
- **JEHAN Robert**
  4 St. Paul's Churchyard, London EC4M 8AY; GB; GB(Residence); GB(Nationality); (Designated only for: IS)

**Inventor(s):**

- **HAYES John William**
  24700 Skyland Road, Los Gatos, CA 95033; US

**Legal Representative:**

- **JEHAN Robert(et al)(commercial rep.)**
  Williams Powell, Morley House, 26-30 Holborn Viaduct, London EC1A 2BP; GB;

| | Country | Number | Kind | Date |
|---|---|---|---|---|
| Patent | WO | 200321436 | A2-A3 | 20030313 |
| Application | WO | 2002GB3968 | | 20020830 |
| Priorities | US | 2001946144 | | 20010904 |

**Designated States:** (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG,
BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD,
GE, GH, GM, HR, HU, ID, IL, IN, IS, JP,
KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT,
LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ,
NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE,
SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ,
UA, UG, UZ, VN, YU, ZA, ZM, ZW

**[EP]** AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;
FI; FR; GB; GR; IE; IT; LU; MC; NL; PT;
SE; SK; TR;

**[OA]** BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;
ML; MR; NE; SN; TD; TG;

**[AP]** GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;
UG; ZM; ZW;

**[EA]** AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

**Language** Publication Language: English
Filing Language: English
Fulltext word count: 11900

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

**Detailed Description:**

...Transmission Control Protocol (TCP) header.

Figure 7 is an illustration which shows the relationship between the network interface NIC, the computer 0 network E and **other primary components** of a computer C including the central processor CPU, the memory controller MC and the memory M.

Figure 8 is an illustration of a classical...specific information about how the content is to be transported from the host computer to the ISP, and then finally to the person requesting the **information**. Much of this I 0 initial request pertains to a determination of the "application protocol" that will be used to convey information from the host...webpage has a limited amount of hardware, software and storage space, and, as a consequence, a limited amount processing capacity that is available for fulfilling **requests** for **information**, files or images from users. User requests are conveyed to a host computer over the Internet. Once they arrive at the host, they are generally...protocol processing tasks, which are normally furnished by the host, are
5
generally delegated to auxiliary processor. These protocol processing tasks generally involve interpreting the **requests** for **data** as they arrive from many users. This new auxiliary processor supports the efforts of the primary hardware and software within the host computer, and may...having to modify the host protocol stack using undefined or undocumented interfaces makes the commercial viability of such a product very limited.

Because the host **protocol** stack is **not** modified, **implementing** selective offloading of **protocol** processing is operating system independent. This means that the architecture described within this docurnent is suitable for a wide range of operating systems. This allows...86, a checksurn 88, and an urgent pointer 90.

Figure 7 illustrates the relationship between the network interface NIC 26, the computer network 14 and **other primary components** of a computer 12, including the central processor 28, the memory controller 106, and the memory 108. The fields of the TCP header are examples...

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

**~~ Non-Patent Literature Abstracts**

13/3,K/5 (Item 3 from file: 56)

0000592113 IP Accession No: 200702-90-009342
**Building a virtual topology atop wireless devices**
Waisbrot, Nathaniel
Journal of Computing Sciences in Colleges , v 17 , n 6 , p 297-298 , May 2002
**Publication Date:** 2002
**Publisher:** Association for Computing Machinery, Inc. , One Astor Plaza, 1515 Broadway , New York , NY , 10036-5701
**Country Of Publication:** USA
**Publisher Url:** http://www.acm.org/
**Publisher Email:** SIGS@acm.org
**Document Type:** Journal Article
**Record Type:** Abstract
**Language:** English
**File Segment:** Computer & Information Systems Abstracts
**Abstract:**
In recent years, networks have become an important topic in the field of computer science. Teaching about networks can be difficult, because it is **not** usually feasible to **configure** and reconfigure a mid-sized or even small network as a teaching tool. The eventual goal of my advisor's grant is to develop classroom... ...not fully connected, primarily to demonstrate routing. My project was to determine the best method to build a virtual topology and simulate various network routing **protocols** on wireless "Cybiko" devices. I wanted to allow the network topology to be changed on the fly, and to simulate nodes dropping off the network... ...make the virtual topology interface general and as abstracted from the Cybiko operating system as possible, so that users could potentially write their own routing **protocols**.Because the project was designed as a teaching tool, I designed a **client**-server system, with the **clients** as the actual nodes, and the server acting as an administrator. The **clients** contact the server to receive initial information about both the topology to use and the other **clients** in the system. The server can announce topology changes to **clients**, or order **clients** to go offline, simulating machine or network failures. While the system is running, the **protocol** code handles user **requests** to send and receive **data**.To reduce traffic over the wireless network, I gave each of the **client** hand-helds a full copy of the topology. This allows them to consult a local table to determine the distance and status of their neighbors, rather than **requesting** the **information** from the **server** or **other** nodes. The local routing table can also be used to determine whether a node is a neighbor, so that attempts to send data to nodes... ...class at Vassar College. The system worked quite well with the topologies we used. The server was able to disconnect and reconnect nodes, and the **clients** were able to use a variety of routing **protocols** to communicate.Although the project now satisfies all of its intended requirements, I am interested in extending it in some areas. Currently, **protocol** code must be compiled into the simulation **application**; using dynamic libraries would not only be more elegant, it would allow the **clients** to switch **protocols** while routing (e.g. to demonstrate the difference between a broken implementation of a **protocol**, and a working one).

**Descriptors:** Networks; Computer simulation; **Clients**; Topology; Computer networks; Routing (telecommunications); **Protocol** (computers); Servers; Teaching; Education; Tools; Wireless communication; Switching theory; Mathematical models; Construction; Tables (data); Reproduction; Failure; Disengaging; **Client** server systems; Traffic flow; Contact; Traffic engineering; Operating systems; Classrooms; Dynamics; Handles; Consultancy

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

services; Grants; Servers (computers)
**Identifiers:**

23/3,K/3 (Item 1 from file: 8)
DIALOG(R)File 8: Ei Compendex(R)

0017432165 **E.I. COMPENDEX No:** 20064710252645
**Update-aware scheduling algorithms for hierarchical data dissemination systems**
**Issue Title:** 7th International Conference on Mobile Data Management, 2006. MDM 2006
Omotayo, Adesola; Hammad, Moustafa A.; Barker, Ken
**Corresp. Author/ Affil:** Omotayo, A.: Department of Computer Science, University of Calgary, Calgary, Alta., Canada
**Corresp. Author email:** omotayo@cpsc.ucalgary.ca
**Author email:** hammad@cpsc.ucalgary.ca; barker@cpsc.ucalgary.ca
**Conference Title:** 7th International Conference on Mobile Data Management, 2006. MDM 2006
**Conference Location:** Nara Japan **Conference Date:** 20060510-20060512
**E.I. Conference No.:** 68564
Proceedings - IEEE International Conference on Mobile Data Management ( Proc. IEEE Int. Conf. Mobile Data Manage. ) ( United States ) 2006 , IEEE P2526 2006/-
**Publication Date:** 20061124
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**ISSN:** 1551-6245 **ISBN:** 0769525261; 9780769525266
**Item Identifier (DOI):** 10.1109/MDM.2006.161
**Article Number:** 1630554
**Document Type:** Conference Paper; Conference Proceeding **Record Type:** Abstract
**Treatment:** T; (Theoretical)
**Language:** English **Summary Language:** English
**Number of References:** 16
Mechanisms to efficiently and effectively transmit up-to- date information to **clients** are of significant interest. Broadcast-based scheduling in hierarchical data dissemination systems are under reported in the literature. In these systems a primaly server accepts updates that are broadcast to **secondaiy servers** and then to a population of **clients** upon **requests**. This paper focuses on **data** dissemination with update propagation at the primaly **server** side. Our **initial** study shows that at high update rates, a straightforward broadcast scheduler that ignores **clients**' access patterns can provide **clients** with outdated information more than 80% of the time. We propose three broadcast scheduling algorithms that primarily differ in how data dissemination with update propagation is guided at the primaly and **secondaiy servers**. We present mechanisms based on real and predicted **clients**' access patterns. We evaluate the new scheduling algorithms by running an extensive set of experiments. The performance study illustrates that the third algorithm, which depends on predictive scheduling at both the primaly and the **secondaiy servers**, provides the best response time and the reception of up-to-date information. (c) 2006 IEEE.
**Descriptors:**

23/3,K/5 (Item 1 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

0003500186 IP Accession No: 20091271895
**Method of masking application processing applied to a request for access to a server, and a corresponding masking system**
Mittig, Karel; Goutard, Cedric; Agostini, Pierre
, USA
**Publisher Url:** http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=7581014.PN.&OS=pn/7581014& RS=PN/7581014
**Document Type:** Patent
**Record Type:** Abstract
**Language:** English
**File Segment:** ANTE: Abstracts in New Technologies and Engineering
**Method of masking application processing applied to a request for access to a server, and a corresponding masking system**
**Abstract:**
A method of and module for masking **application** processing applied to a **request** for access to a server by a **client** workstation connected via **successive proxy servers**. The **application** of a **first proxy server**, is executed, the address of the **client** workstation is inserted into a specific **data** field of the **access request** message header, without calling for any IP spoofing function and the access **request** message for execution of successive **application** processing is sent to **successive proxy servers**. After execution of its **application** processing by a last proxy server and transmitting of the access **request** message to the server, the access **request** message is intercepted at a masking module, the specific field from the header is eliminated to mask the **application** processing, and a masked access **request** message is constructed and the masked access **request** message is sent from the masking module to the server.
**Descriptors:** Servers; Messages; Masking; Proxy **client** servers; Modules; Workstations; Headers; IP (Internet Protocol); Transmission; Construction specifications; Masks; Spoofing
**Identifiers:**

23/3,K/7 (Item 3 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0002967361 IP Accession No: 20090506277
**Securing audio-based access to application data**
Ingerman, Aleksandr; Jones, Bruce Cordell; Millett, Thomas W
, USA
**Publisher Url:** http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=7484102.PN.&OS=pn/7484102& RS=PN/7484102
**Document Type:** Patent
**Record Type:** Abstract
**Language:** English
**File Segment:** ANTE: Abstracts in New Technologies and Engineering
**Securing audio-based access to application data**
**Abstract:**
The present invention extends to methods, systems, and computer program products for securing audio-based **access** to **application data**. A **client** sends and a server receives a **request** for audio-based **access** to **application data**. The **server** sends a **first** audio challenge for a user credential in response to the **request**. The **client** receives the first

audio challenge and sends a user credential. The server receives the user credential and sends a second audio challenge. The second audio challenge is configured to be understandable to a user of the **client** but difficult to recognize using automated voice recognition techniques. The **client** receives the second audio challenge and sends an additional portion of data responsive to the second audio challenge. The **server** receives the **additional** portion of data and calculates a **client** authorization based on the received user credential and received additional portion of data.

23/3,K/11 (Item 7 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0001941808 IP Accession No: 20081900743
**Method and apparatus for session replication and failover**
Pullara, Sam; Halpern, Eric M; Peddada, Prasad; Messinger, Adam; Jacobs, Dean Bernard
, USA
**Publisher Url:** http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u
=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=74
09420.PN.&OS=pn/7409420& RS=PN/7409420
**Document Type:** Patent
**Record Type:** Abstract
**Language:** English
**File Segment:** ANTE: Abstracts in New Technologies and Engineering
**Abstract:**
...replication system provides real-time data replication without unnecessarily slowing down the user experience. A system in accordance with the present invention may utilize a **primary server** to serve **requests** from a network **client**, as well as a **secondary server** to replicate the session **information**. When a **request** is received on the session, an attempt may be made to serve the **request** on the **primary server**. If the **primary** is unable to receive or respond to the **request**, the **request** may be served on the **secondary application server** or on a new **primary server**. If the **secondary server** receives the **request**, the **secondary server** may become the new **primary server**. If a new **primary server** is selected, the new primary may **request** the session **information** from the **secondary server**.
**Descriptors:** Servers; Replication; Servers (computers); Retarding; **Application** servers; Inventions; United States; Real time; Networks; Data replication
**Identifiers:**

23/3,K/12 (Item 8 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0001929633 IP Accession No: 20081907196
**Method for PC client security authentication**
Lin, Haitao; Gan, Quan; Chen, Shuiyang; Wang, Xiaolan
, USA
**Publisher Url:** http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u
=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=74
18727.PN.&OS=pn/7418727& RS=PN/7418727
**Document Type:** Patent
**Record Type:** Abstract
**Language:** English

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

**File Segment:** ANTE: Abstracts in New Technologies and Engineering
**Method for PC client security authentication**
**Abstract:**
A security authentication for PC **client** is provided according to the present invention, wherein said method includes: PC **client** sends a registry **request** to a server with a user ID and a password; The **server** makes **first** authentication based on the user ID and password, if the authentication succeeds, a field used for re-authentication will be created and returned to the PC **client** through an authentication successful message; When initiating a call, the PC **client** transmits the user ID and the field used for re-**authentication acquired** when registered to media gateway controller; The media gateway controller transfers the user ID and field used for re-authentication to the **server**, which makes **second** authentication according to the user ID and the field used for the second authentication, if the authentication fails, the call will be rejected, otherwise the...

23/3,K/13 (Item 9 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0001439717 IP Accession No: 20080922030
**Method for providing information to a web server**
Brandrud, Knut; Schuba, Marko; Zavagli, Guido
, USA
**Publisher Url:** http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=7380013.PN.&OS=pn/7380013& RS=PN/7380013
**Document Type:** Patent
**Record Type:** Abstract
**Language:** English
**File Segment:** ANTE: Abstracts in New Technologies and Engineering
**Abstract:**
**Access** to **information** related to a **client** terminal is provided to a **first** web **server**, the information being stored by a **second** web **server**. The **first** web **server** is connected to the **client** terminal via a **proxy server**. The **second** web **server** sends a message, including a cookie, to the proxy server, wherein the cookie comprises a network address of the **second** web **server**. The cookie, related to the **client** terminal, is stored in the proxy server. The proxy server receives a message from the **client** terminal addressed to the **first** web **server** and the proxy server inserts the stored cookie into the received message. The proxy server forwards the received message to the **first** web **server**, which uses the cookie to **request information** from the **second** web **server**.
**Descriptors:** Servers (computers); World Wide Web; Servers; Proxy **client** servers; Heating; Terminals; Messages; Inserts; Networks
**Identifiers:**

23/3,K/14 (Item 10 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0001347820 IP Accession No: 20081036141
**Fault tolerant NFS server system and mirroring protocol**
Kandasamy, David R; Butler, Mitchel B; Foss, Andrew L; Peterson, Bradley M; Patwardhan, Chintamani M; Ribble, Michael T; Rothmeier, Dieter; Ramil, Gaudencio
, USA

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

**Publisher Url:** http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=5513314.PN.&OS=pn/5513314& RS=PN/5513314
**Document Type:** Patent
**Record Type:** Abstract
**Language:** English
**File Segment:** ANTE: Abstracts in New Technologies and Engineering
**Abstract:**
A network computer system providing for the fault tolerant storage and retrieval of data files includes a **client** system connected to a data communication network that may source a first **data** transfer **request** to said **data** communication network for the transfer or retrieval of data. A **first server** system, including **first** medium for storing data files, is connected to the data communication network so as to be responsive to first **data** transfer **requests**. A **second server** system, including **second** medium for storing data files is also connected to said data communication network to also be responsive to first **data** transfer **requests**. A control protocol, established between the **first** and **second server** systems, coordinates an asymmetric response by the **first** and **second server** systems to a first **data** transfer **request**, such that file **data** transferred by the **client** with the first **data** transfer **request** is replicated to the first and second storing mediums and such that file data transferred to the **client** system in response to the first data transfer is non-replicatively provided to the **client** system by either the **first** or **second server** system.

23/3,K/15 (Item 11 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0000983654 IP Accession No: 2008499380
**System for adding requested document cross references to a document by annotation proxy configured to merge and a directory generator and annotation server**
van Hoff, Arthur A
, USA
**Publisher Url:** http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=5822539.PN.&OS=pn/5822539& RS=PN/5822539
**Document Type:** Patent
**Record Type:** Abstract
**Language:** English
**File Segment:** ANTE: Abstracts in New Technologies and Engineering
**System for adding requested document cross references to a document by annotation proxy configured to merge and a directory generator and annotation server**
**Abstract:**
In a distributed computer system, an automated document annotation system and method adds hypertext cross-references to a set of known **information** sources into documents **requested** by a **client** computer in such a way that the merged document is displayable by existing Web browsers. The distributed computer network incorporates a plurality of servers to store documents. Each stored document has a unique document identifier and is viewable from a **client** computer having a browser configured to **request** and receive documents over the network. An annotation proxy, which is a software procedure configured to merge a **requested** document from a **first server** with hypertext links to documents containing associated supplemental information. The set of hypertext links and criteria for identifying

where such links should be added to **requested** documents are defined by one or more dictionaries of cross-references. The annotation proxy then relays the merged document to a receiver unit that is selected from **another proxy**, such as a firewall **proxy** or **another** annotation overlay **proxy**, or the browser, which ultimately displays the merged document. The annotation proxy optionally includes a dictionary generator that generates a dictionary of references to documents **requested** by the user, each reference in the dictionary indicating the textual context of the hypertext link or links used to **request** the associated document. The generated dictionary represents information sources known and used by the user. The annotation proxy then annotates **requested** documents with cross-references in the dictionary that was generated by the annotation proxy.
**Descriptors:** Proxy **client** servers; Hypertext; Servers; Generators; Directories; Computer programs; Firewalls; Receivers; Software; Servers (computers); Sun ; Networks; Computer networks
**Identifiers:**

23/3,K/16 (Item 12 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0000839408 IP Accession No: 2008493259
**Dynamic server switching for maximum server availability and load balancing**
Gehr, Chuck Royal; Von Behren, Paul David; Williams, Michael Patrick; Wood, Robert Barry
, USA
**Publisher Url:** http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=5828847.PN.&OS=pn/5828847& RS=PN/5828847
**Document Type:** Patent
**Record Type:** Abstract
**Language:** English
**File Segment:** ANTE: Abstracts in New Technologies and Engineering
**Abstract:**
The dynamic server switching system maintains a list in each **client** which identifies the **primary server** for that **client** and the preferred communication method as well as a hierarchy of successively **secondary servers** and communication method pairs. In the event that the **client** does not have **requests** served by the designated **primary server** or the designated communication method, the system traverses the list to ascertain the identity of the **first** available alternate **server** -communication method pair. The **client** then uses this retrieved **data** to initiate future **requests**. The **client** periodically tests the **primary server**-communication method pair to determine whether the fault has been cleared. If so, the **client** reestablishes the originally selected **primary server**-communication method pair as the **request** route. This system dynamically load balances in the face of failures, handles transient faults and can use a neuromorphic processing element to monitor system activity...

23/3,K/17 (Item 13 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0000615766 IP Accession No: 2008291979
**Common session token system and protocol**
Kunzelman, Kevin; Hutto, Sterling
, USA

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

**Publisher Url:** http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=60 41357.PN.&OS=pn/6041357& RS=PN/6041357
**Document Type:** Patent
**Record Type:** Abstract
**Language:** English
**File Segment:** ANTE: Abstracts in New Technologies and Engineering
**Abstract:**
An improved session control method and apparatus includes a **client** which establishes a session with a **first server** such that the **first server** can identify the **client**. When the **client** wishes to migrate from the **first server** to a **second server**, the **client requests** a session token from the **first server**. The session token is a data element generated by the **first server** which is unique over the **client**-server network being navigated and identifies the particular session with the **first server**. The session token is preferably a difficult to forge data element, such as a data element digitally signed using the private key of the **first server**. The session token is passed from the **client** to the **second server** to initiate migration to the **second server**. If session data is too bulky to be passed as part of the session token, the **second server** may use data from the session token to formulate a **request** to the **first server** for **additional data needed** to handle the state of the session. To minimize the transmission of data, the **second server** might maintain a version of the bulk session **data** and only **request** an update to the version of the data indicated in the session token.

23/3,K/18 (Item 14 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0000474032 IP Accession No: 2008171471
**Clustered file management for network resources**
Wolff, James J
, USA
**Publisher Url:** http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=61 01508.PN.&OS=pn/6101508& RS=PN/6101508
**Document Type:** Patent
**Record Type:** Abstract
**Language:** English
**File Segment:** ANTE: Abstracts in New Technologies and Engineering
**Abstract:**
Methods for operating a network as a clustered file system is disclosed. The methods involve **client** load rebalancing, distributed Input and Output (I/O) and resource load rebalancing. **Client** load rebalancing refers to the ability of a **client** enabled with processes in accordance with the current invention to remap a path through a plurality of nodes to a resource. Distributed I/O refers... ...of nodes to resources. Resource rebalancing includes remapping of pathways between nodes, e.g. servers, and resources, e.g. volumes/file systems. The network includes **client** nodes, server nodes and resources. Each of the resources couples to at least two of the server nodes. The method for operating comprising the acts of: **redirecting** an I/O **request** for a resource from a **first server** node coupled to the resource to a **second server** node coupled to the resource; and splitting the I/O **request** at the **second server** node into an **access** portion and a **data** transfer portion and passing the access portion to a corresponding administrative server node for the resource, and completing at the **second server** nodes **subsequent** to receipt of an access

grant from the corresponding administrative server node a data transfer for the resource. In an alternate embodiment of the invention...

10655368 Method for Access by Server-Side Components using Unsupported Communication Protocols Through Passthrough Mechanism - Results

**~~ Non-Patent Literature Full-Text**

13/3,K/1 (Item 1 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

0023631213 **Supplier Number:** 178400974 (USE FORMAT 7 OR 9 FOR FULL TEXT )
**Invisible links revolutionize industrial communications: with wireless becoming more practical, secure, and reliable, you can throw the cost of wiring out the factory window.(technology report)**
Frenzle, Louis E.
Electronic Design , 56 , 7 , 41(5)
April 10 , 2008
ISSN: 0013-4872
**Language:** English
**Record Type:** Fulltext
**Word Count:** 3232 **Line Count:** 00266
...of chip suppliers have made 802.11 viable even in sensor or actuator applications, where long battery life is essential for minimum maintenance.

When your **data**-transport **application needs** high speed and long range, it becomes an excellent choice. It also matches up nicely with the corporate office LAN. The 802.11i security standard...
...current popular industrial networking technologies like HART, Foundation Fieldbus, Modbus, Profibus, and Common Industrial Protocol (CIP).

One big problem is that 802.15.4 does **not support** the Internet **Protocol**, so you need specialized **gateways** or **other** solutions to connect to the Internet. One potential solution is to use a new standard developed by the Internet Engineering Task Force (IETF) known as...

13/3,K/3 (Item 1 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

01346416 **Supplier Number:** 08012188 **(Use Format 7 Or 9 For** FULL TEXT )
**Simplifying complex Windows development through the use of a client-server architecture. (tutorial)**
Kerber, Scott
Microsoft Systems Journal , v5 , n1 , p21(14)
Jan , 1990
**Document Type:** tutorial
ISSN: 0889-9932
**Language:** ENGLISH **Record Type:** FULLTEXT; ABSTRACT
**Word Count:** 5293 **Line Count:** 00426
...discardable segments) and permits several large applications to run simultaneously (bank switching).

Specializing protocols can be defined through Windows support of user-definable message types. **Request** and response **data** are passed between **client** and server via memory blocks allocated from the Windows global heap.

Messages under Windows are usually sent to other windows. A receiving window may reside...

...a request to a server, it must first put its request into a packet. A

packet is usually a buffer that the client allocates. The **client** fills the buffer with the **data required** to make the **request**. The **data** must be in a format previously agreed upon between client and server. When ready, the client executes a network send primitive (typically a function call...

...Both client and server can allocate and use a single block of nonbanked memory for request and response data. WinTrieve uses nonbanked memory to communicate **request** and response **data** with **client applications**. A sample WinTrieve client-server memory map is shown in Figure 7.

The second way that global memory can be allocated is with the GMEM ...

...frame EMS) for the client-server that communicates using GMEM SHARE global memory blocks. The figure shows the server mapped into memory to service a **client request**. The **request data** packet, allocated by the **client**, contains the appropriate **request data**. The global memory handle of the **request data** packet was passed by the **client** to the server when the request message was sent. To send the request message, the client calls the Windows function SendMessage. When the server calls...Books Browser. Before existing, Books Browser terminates the connection by sending a terminate connection message to WinTrieve. WinTrieve then return a terminate acknowledgment.

The WinTrieve **Protocol**

The synchronous **protocol implemented** for WinTrieve is **not** WinTrieve-dependent. It should be relatively straightforward to implement for **other server** applications. Code samples, although taken from WinTrieve, have been rewritten to minimize or completely remove WinTrieve-specific details.

The WinTrieve protocol supports three message types...